## CLAIMS

1. A method, comprising:

generating a first set of integrity information for a first processing system;

sending said first set of integrity information to a second processing system; and

generating an attestation value for said first processing system by said second processing system using said first set of integrity information.

2. The method of claim 1, wherein generating said first set of integrity information comprises:

selecting an application from a plurality of applications to be executed by said first processing system; and

generating said first set of integrity information for said application using a cryptographic algorithm.

3. The method of claim 1, wherein generating said attestation value comprises:

retrieving a second set of integrity information for said first processing system;

comparing said first set of integrity information with said second set of integrity information; and

generating said attestation value in accordance with said comparison.

4. The method of claim 1, wherein said sending comprises:

encrypting said integrity information using a first key for said first processing system; and

sending said encrypted integrity information to said second processing system.

5. The method of claim 4, further comprising authenticating said integrity information prior to generating said attestation value.

6. The method of claim 5, wherein said authenticating comprises:

receiving said encrypted integrity information;

retrieving a second key for said first processing system; and

decrypting said encrypted integrity information using said second key.

7. A method, comprising:

generating a first set of integrity information for a first process;

sending said first set of integrity information to a second process; and

generating an attestation value for said first process by said second process using said first set of integrity information.

8. The method of claim 7, wherein said first process and said second process are executed by different processing systems.

9. A system, comprising:

an antenna;

a transceiver to connect to said antenna;

a first processing system to connect to said transceiver, said first processing comprising a plurality of applications;

a second processing system to connect to said transceiver and said first processing system; and

a dynamic attestation module to connect to said first and second processing systems, said second processing system to perform dynamic attestation for one of said applications to be executed by said first processing system using said dynamic attestation module.

10. The system of claim 9, wherein said dynamic attestation module comprises an integrity module to generate a first set of integrity information for said application.

11. The system of claim 10, wherein said dynamic attestation module retrieves a second set of integrity information for said application.

12. The system of claim 11, wherein said dynamic attestation module comprises an attestation module to generate an attestation value for said application by comparing said first set of integrity information with said second set of integrity information.

13. The system of claim 10, wherein said dynamic attestation module comprises an authentication module to authenticate said first set of integrity information.

14. The system of claim 12, wherein said second processing system communicates control signals to said transceiver, said second processing system to disable access to said transceiver by said first processing system in accordance with said attestation value.

15. An apparatus, comprising:

a first processing system comprising a plurality of applications;

a second processing system to connect to said first processing system; and

a dynamic attestation module to connect to said first and second processing systems, said second dynamic attestation module to perform dynamic attestation for one of said applications.

16. The apparatus of claim 15, wherein said dynamic attestation module comprises an integrity module to generate a first set of integrity information for said application.

17. The apparatus of claim 16, wherein said dynamic attestation module retrieves a second set of integrity information for said application.

18. The apparatus of claim 17, wherein said dynamic attestation module comprises an attestation module to generate an attestation value for said application by comparing said first set of integrity information with said second set of integrity information.

19. The apparatus of claim 16, wherein said dynamic attestation module comprises an authentication module to authenticate said first set of integrity information.

20. An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a processor, are operable to generate a first set of integrity information for a first processing system, send said first set of integrity information to a second processing system, and generate an attestation value for said first processing system by said second processing system using said first set of integrity information.

21. The article of claim 20, wherein the stored instructions, when executed by a processor, generate said first set of integrity information using stored instructions operable to select an application from a plurality of applications to be executed by said first processing system, and generate said first set of integrity information for said application using a cryptographic algorithm.

22. The article of claim 20, wherein the stored instructions, when executed by a processor, generate said attestation value using stored instructions operable to retrieve a second set of integrity information for said first processing system, compare said first set of integrity information with said second set of integrity information, and generate said attestation value in accordance with said comparison.